CHAPTER 8

Intelligence, Counterintelligence, and Security Support

8.0 Chapter Overview

8.0.1. Purpose

The purpose of this chapter is two-fold: 1) to focus Program Manager attention on and describe Program Manager responsibilities regarding the prevention of inadvertent technology transfer of dual-use and leading edge military technologies that support future defense platforms and DoD capabilities-based military strategies; and, 2) to provide guidance and describe support available for protecting those technologies.

8.0.2. Contents

This Chapter is divided into six sections as follows:

Section 8.0, Chapter Overview, provides the purpose of this chapter, briefly summarizes the content and organization, and provides a brief discussion on applicability.

Section 8.1, Introduction, ranges from section 8.1.1 to section 8.1.2. It provides an overview of protection considerations, and addresses the planning, legal issues, and information reporting associated with the DoD Research and Technology Protection (RTP) effort.

Section 8.2, Intelligence, ranges from section 8.2.1 to section 8.2.2. It contains information on intelligence support to acquisition programs and intelligence supportability.

Section 8.3, Pre-Acquisition Protection Strategy for RDT&E Activities, ranges from section 8.3.1 to section 8.3.4. It covers procedures for RTP at RDT&E facilities.

Section 8.4, Acquisition Protection Strategy for Program Managers, ranges from section 8.4.1 to section 8.4.11.2. It contains procedures for protecting acquisition program technologies and information.

Section 8.5, Specialized Protection Processes, ranges from section 8.5.1 to section 8.5.6.2. It describes procedures in system security engineering, counterintelligence (CI), anti-tamper (AT), information assurance, horizontal analysis and protection, and RTP assessments and inspections that apply to protection activities, both at RDT&E sites and within acquisition programs.

8.0.3. Applicability

This chapter describes procedures for identifying and protecting DoD research and technologies, to include designated science and technology information (DS&TI) and critical program information (CPI), in accordance with DoD Directive 5000.1, DoD Instruction 5000.2, DoD Directive 5200.39, and DoD 5200.1-R. DS&TI and CPI are defined in DoD Directive 5200.39 and in section 8.1.1.

The guidance applies to all activities, phases, and locations (to include contractor locations) where DS&TI and CPI are developed, produced, analyzed, maintained, employed, transported, stored, or used in training, as well as during its disposal.

This Chapter does not apply to acquisitions by the DoD Components that involve a special access program (SAP) created under the authority of E.O. 12958. The unique nature of SAPs requires compliance with special security procedures of DoD Directive O-5205.7. If the program or system contains CPI, the SAP Program Manager will prepare and implement a Program Protection Plan (PPP) prior to transitioning to collateral or unclassified status. Security, intelligence, and CI organizations should assist the SAP Program Manager in developing the PPP. The PPP will be provided to the offices responsible for implementing protection requirements before beginning the transition.

8.0.4. Documents Discussed in Chapter 8

The documents discussed in Chapter 8 are listed below in Table 8.0.4.1. This table lists the documents that are prepared when the program manager or RDT&E site director determines they are necessary, and includes identification of and electronic links to the sections of Chapter 8 that contain the guidance for the preparation of each document.

Table 8.0.41. Documents Discussed in Chapter 8

Document	Prepare if:	Discussion on Preparation
Program Protection Plan (PPP)	The acquisition program has Critical Program Information (CPI)	8.4.6. DoDD 5200.39
Technology Assessment/Control Plan (TA/CP)	The acquisition program may have, or will have, foreign participation	8.4.3. DoDD 5530.3
Delegation of Disclosure Authority Letter (DDL)	The acquisition program has foreign participation	8.4.8.3. DoDD 5530.3
Counterintelligence Support Plan (CISP)	- For all major RDT&E activities and - For an acquisition program with Critical Program Information (CPI)	8.3.1.2. 8.3.2.1. 8.3.4. 8.5.2.
Multidiscipline CI (MDCI) Threat Assessment	The program has Critical Program Information; the MDCI threat assessment is prepared by the supporting CI activity	8.4.6.2. 8.4.7.
Security Classification Guide (SCG)	The program contains classified information or controlled unclassified information	8.4.6.5. DoD 5200.1-R 8.4.6.5.
System Security Authorization Agreement (SSAA)	System Security Authorization Agreement (SSAA) defined in paragraph 7.5.12.	8.5.4. Chapter 8
System Security Management Plan (SSMP)	the program manager chooses to use a SSMP to plan the program's system security effort	8.5.1.1. 8.5.1.2.
Anti-Tamper Plan	AT measures are applied	8.5.3.3.

		8.5.3.1.
Information Exchange Agreements	The acquisition program has foreign participation	8.3.2.2. 8.4.3.
Program Protection Implementation plan (PPIP)	the program manager decides to use a PPIP as part of the contract	8.4.9.3.
DD Form 254, DoD Contract Security Classification Specification	When the program manager includes security controls within the contract or the contract will involve classified information.	8.4.9.7. DoD 5220.22-M

8.0.5. Support from Functional Offices

To properly accomplish activities described in this chapter, the Program Manager needs the cooperation and support of related functional offices. Support to the acquisition community from the intelligence, counterintelligence, and security communities involves a number of staff organizations and support activities that may be unfamiliar to members of the acquisition community. Table 8.0.5.1. lists the functional offices that may support the program manager in various tasks discussed in Chapter 8. This table identifies (and links to) the sections of Chapter 8 that describe various situations involving these offices. The individual assigned responsibility for coordinating intelligence support, counterintelligence support, or Research and Technology Protection (RTP) within a program office, laboratory, T&E center, or other RDT&E organization should identify the proper contacts in these organizations prior to initiating program planning.

Table 8.0.5.1. Functional Offices Discussed in Chapter 8

Functional Offices	Chapter 8 References
Security Support Office • Protection Planning For RDT&E Activities • Assignments, Visits, and Exchanges of Foreign Representatives • Collaboration • Foreign Collection Threat • Execution of the PPP	8.3.2.1. 8.3.2.2 8.4.5.2 8.4.6.2 8.4.11
Counterintelligence Support Organization • Counterintelligence Support During Pre-Acquisition • Collaboration • Multidiscipline CI (MDCI) Threat Assessment • Execution of the PPP • Counterintelligence Support Plan	8.3.4. 8.4.5.2. 8.4.6.2. 8.4.7. 8.4.11 8.5.2
Foreign Disclosure Officer • Safeguarding DoD RDT&E Information • Programs with Foreign Participation	8.3.1.2. 8.4.3. 8.4.5.2. 8.4.8. 8.4.9.6.

• Collaboration • Technology Assessment / Control Plan (TA/CP) • Providing Documentation to Contractors	
Intelligence Support Organization • Intelligence	8.2.
Intelligence Requirements Certification Office • Intelligence Certification	8.2.2.
Government Industrial Security Office • Support from Cognizant Government Industrial Security Offices	8.4.9.7.
Anti-Tamper Support Organization • Anti-Tamper	8.5.3.
DoD Executive Agent for Anti-Tamper • Anti-Tamper	8.5.3.
Operations Security (OPSEC) • Collaboration	8.4.5.2.
Defense Security Service • Counterintelligence Support During Pre-Acquisition	8.3.4.

8.1. Introduction

8.1.1. General Information

The DoD actively seeks to include allies and friendly foreign countries as partners in the research, development, test and evaluation (RDT&E); production; and support of defense systems. The Department of Defense encourages early involvement with allied and friendly foreign partners. Such cooperative foreign government partnerships should begin at the requirements definition phase, whenever possible. Successful execution of cooperative programs will promote the desirable objectives of standardization, commonality, and interoperability. The U.S. Government and its foreign government partners in these endeavors will benefit from shared development costs, reduced costs realized from economies of scale, and strengthened domestic industrial bases. Similarly, the DoD plays a key role in the execution of security cooperation programs that

ultimately support national security objectives and foreign policy goals. U.S. defense system sales are a major aspect of security cooperation.

Increasingly, the U.S. Government relies on sophisticated technology in its defense systems for effectiveness in combat. Further, technology is recognized as a force multiplier and will continue to improve the warfighter's survivability. Therefore, it is not only prudent, but also practical to protect technologies deemed so critical that their exploitation will diminish or neutralize a U.S. defense system's effectiveness. Protecting critical technologies preserves the U.S. Government's research and development resources as an investment in the future, rather than as an expense if technology is compromised and must be replaced prematurely. It also enhances U.S. industrial base competitiveness in the international marketplace.

When necessary and successfully applied, procedures and guidance in this chapter are designed to protect Designated Science and Technology Information (DS&TI) and Critical Program Information (CPI) against compromise, from RDT&E throughout the acquisition life cycle (including property disposal), at all involved locations or facilities. DS&TI is research and technology classified information and research and technology CUI identified by RDT&E site directors to receive specialized CI and security support. CPI, in an acquisition program, may be classified information or CUI about technologies, processes, applications, or end items that if disclosed or compromised, would degrade system combat effectiveness, compromise the program or system a\capabilities, shorten the expected combat effective life of the system, significantly alter program direction, or require additional research, development, test, and evaluation resources to counter the impact of the compromise. CPI includes, but is not limited to, CPI inherited from another program and CPI identified in pre-system acquisition activities or as a result of non-traditional acquisition techniques (e.g., Advanced Concept Technology Demonstration, flexible technology insertion).

- The teamwork engendered by this chapter provides intelligence support to the analysis phase of capabilities integration and development prior to Milestone A. The teamwork also selectively and effectively applies research and technology protection (RTP) countermeasures and counterintelligence (CI) support to the program, resulting in cost-effective activities, consistent with risk management principles, to protect DS&TI as well as CPI.

- Anti-Tamper (AT) techniques and application of system security engineering (SSE) measures allow the United States to meet foreign customer needs for advanced systems and capabilities while ensuring the protection of U.S. technological investment and equities. AT techniques and SSE measures are examples of protection methodologies that DoD programs use to protect critical system technologies.

8.1.2. Protection Overview

DS&TI and CPI may include classified military information, which is considered a national security asset that will be protected and shared with foreign governments only when there is a clearly defined benefit to the United States (see DoD Directive 5200.39). It may also include Controlled Unclassified Information (CUI), which is official

unclassified information that has been determined by designated officials to be exempt from public disclosure, and to which access or distribution limitations have been applied in accordance with national laws and regulations. It may also include unclassified information restricted by statute, such as export controlled data.

Both DS&TI and CPI require protection to prevent unauthorized or inadvertent disclosure, destruction, transfer, alteration, reverse engineering, or loss (often referred to as "compromise").

DS&TI should be safeguarded to sustain or advance the DoD technological lead in the warfighter's battle space or joint operational arena.

The CPI, if compromised, will significantly alter program direction; result in unauthorized or inadvertent disclosure of the program or system capabilities; shorten the combat effective life of the system; or require additional research, development, test, and evaluation (RDT&E) resources to counter the impact of its loss. See DoD Directive 5200.39 for DS&TI and CPI definitions.

The theft or misappropriation of U.S. proprietary information or trade secrets, especially to foreign governments and their agents, directly threatens the economic competitiveness of the U.S. economy. Increasingly, foreign governments, through a variety of means, actively target U.S. businesses, academic centers, and scientific developments to obtain critical technologies and thereby provide their own economies with an advantage. Industrial espionage, by both traditionally friendly nations and recognized adversaries, proliferated throughout the 1990s.

Information that may be restricted and protected is identified, marked, and controlled in accordance with DoD Directives 5230.24 and 5230.25 or applicable national-level policy and is limited to the following:

- Information that is classified in accordance with Executive Order 12958, and

- Unclassified information that has restrictions placed on its distribution by:

- U.S. Statutes (e.g., Arms Export Control Act, Export Administration Act);

- Statute-driven national regulations (e.g., Export Administration Regulations, International Traffic in Arms Regulations); and

- Related national policy (e.g., Executive Order 12958, National Security Decision Directive 189).

Incidents of loss, compromise, or theft of proprietary information or trade secrets involving DS&TI and CPI, are immediately reported in accordance with Section 1831 et seq. of Title 18 of the United States Code, DoD Instruction 5240.4, and DoD Directive 5200.1. Such incidents are immediately reported to the Defense Security Service (DSS), the Federal Bureau of Investigation (FBI), or the applicable DoD Component CI and law enforcement organizations. If the theft of trade secrets or proprietary information might reasonably be expected to affect DoD contracting, DSS should notify the local office of the FBI.

8.2. Intelligence

8.2.1. Threat Intelligence Support

Acquisition programs should be supported by a current and validated threat assessment provided by the Defense Intelligence Agency (DIA) or Service Intelligence Production Centers. Major Defense Acquisition Programs are required to utilize DIA-validated threat assessments to support program development in accordance with DoD Directive 5105.25. These threat assessments can take the form of:

- A Capstone document that addresses current and future threats to a defined U.S. warfighting capability; or

- A system-specific threat assessment for programs subject to Defense Acquisition Board review.

The Defense Intelligence Community should maintain continuous contact with the acquisition community to ensure awareness of developing threat information. Program managers should identify Critical Foreign Capabilities that could adversely impact on operational utility or employment of their system.

8.2.1.1. Capstone Threat Assessment

Capstone Threat Assessments should address current and future (10- and 20-year projections) foreign developments that challenge U.S. warfighting capabilities (i.e., precision strike warfare, undersea warfare, space operations, surveillance, and reconnaissance). Since most Capstone Threat Assessments require input from multiple Defense Intelligence elements, DIA edits and integrates the inputs into a single, coherent validated document.

8.2.1.2. System-Specific System Threat Assessment

DIA provides validation for System Threat Assessments, prepared by the appropriate Service, to support major defense acquisition programs. Appropriate Defense Intelligence organization(s), identified by DIA, prepare the System Threat Assessment. The assessment should be kept current and validated. The assessment should be system specific to the degree of system definition available at the time the assessment is being prepared. The assessment should address projected adversary capabilities at system IOC and at IOC plus 10 years. The recommended System Threat Assessment format includes the following elements:

- An executive summary that includes key intelligence judgments and significant changes in the threat environment;

- Discussion of the operational threat environment, adversary capability(s) that may effect operation of the system, system specific threat, reactive threat, and technologically feasible threats. Reference to the Capstone Threat Assessments will be made where possible to streamline the System Threat Assessment;

- A section that addresses developments related to the program manager's Critical Foreign Capabilities; and

- A section that identifies intelligence gaps related to the Critical Foreign Capabilities or of a more over-arching nature.

8.2.1.3. Threat Validation

For MDAPs subject to DAB review, DIA provides validation for System Threat Assessments. DIA validation ensures that all relevant data is considered and appropriately used by author(s) of the assessment.

DIA may also validate other threat information. DIA must validate threat information contained in Joint Capabilities Integration and Development System documents in accordance with Joint Staff guidance.

8.2.1.4. Support to Test and Evaluation

The TEMP should define specific intelligence requirements to support program test and evaluation. DIA should coordinate with the entire Defense Intelligence Community to provide appropriate intelligence support to the Test and Evaluation Community.

8.2.2. Intelligence Certification

DoD Instruction 4630.8 requires the Joint Staff to provide ASD(NII) with an intelligence certification of Information Support Plans (ISPs). The J-2 element of the Joint Staff will facilitate the Intelligence Certification with collaborative inputs from DoD Components. Program managers should be aware of the requirements for Intelligence Certification, and should ensure that ISP preparation considers the certification criteria outlined below.

Overarching Criteria . The Intelligence Certification evaluates intelligence information requirements in ISPs for completeness, supportability, and impact on joint intelligence strategy, policy, and architectural planning. General descriptions of these criteria categories follow:

- **Completeness** . Completeness refers to the extent to which the ISP addresses requirements *for* intelligence support (such as analytical products required, targeting support, imagery, etc.) and program compliance with requirements *by* intelligence (such as interoperability with intelligence systems, compliance with intelligence security standards, etc.).

- **Supportability** . Supportability refers to the availability, suitability, and sufficiency of the required intelligence support. Intelligence Certification analysts will compare a program's stated or derived intelligence support needs with the expected intelligence capabilities that are projected throughout a program life cycle. The ability to adequately assess supportability depends upon the completeness of support requirement declaration.

- **Impact on Intelligence Strategy, Policy, and Architecture Planning** . Impact, within this context, refers to the identification of additional inputs to or outputs from the intelligence infrastructure. Requirements for intelligence support may be transparent with regard to the intelligence support infrastructure if planned products, information, or services are already projected to be available, suitable, and sufficient throughout a program life cycle. In other cases, programs may require new types of support or have increased standards for existing support. These additional inputs or outputs may require changes across the Doctrine, Organization, Training and Education, Materiel, Logistics, Personnel, or Facilities

(DOTMLPF) spectrum. These potential changes impact intelligence strategy, policy, and architecture planning. The impact assessment provides a mechanism for providing critical feedback to the defense and national intelligence communities to highlight potential shortfalls in current or planned intelligence support.

Additional Criteria. The certification also evaluates intelligence-related systems with respect to open system architecture, security, and intelligence interoperability standards. (J-6 Interoperability certification is conducted in a separate, but related process, and is documented in CJCSI 6212.01.)

Those personnel with a Joint Worldwide Intelligence Communications System terminal can access the specific procedures and criteria for the Intelligence Certification on the Intelligence Requirements Certification Office homepage (under "Certification Process"). By telephone, additional information may be obtained by calling the Intelligence Requirements Certification Office at 703- 695-4693.

8.3. Pre-Acquistion Protection Strategy for RDT&E Activities

8.3.1. General

Protection may apply to all seven subcategories of RDT&E (see DoD 7000.14-R, Volume 2B). DoD Directive 5200.39 recognizes the normally unrestricted nature of fundamental research, as identified in National Security Decision Directive (NSDD) 189, and as further stipulated for Basic Research in Executive Order 12958. The term "fundamental research" refers generally to Basic Research (6.1) and Applied Research (6.2), and is defined in the International Traffic in Arms Regulations (ITAR).

8.3.1.1. Purpose

The purpose of pre-acquisition protection is to prevent unauthorized disclosure of DoD RDT&E information. CI and security specialists provide a wide range of services to ensure personnel assigned to RDT&E sites are aware of threats from foreign intelligence services, other foreign interests, or anyone involved in unauthorized acquisition of DoD information. For example, one of these services can be to ensure requirements for authorized foreign involvement are met and that personnel administering such programs are well versed in those requirements.

8.3.1.2. Safeguarding DoD RDT&E Information

Working together, RDT&E laboratories and centers, and CI, security, foreign disclosure, OPSEC, and intelligence organizations should use an interactive process (such as an IPT) to safeguard DS&TI from compromise in order to sustain or advance the DoD technological lead in the future battle space.

The RDT&E commanding officer, site director, or their designee (referred to hereafter as "site director") identifies and prioritizes their DS&TI, and communicates the results to CI, security, foreign disclosure, operations security (OPSEC), and intelligence organizations.

- The site director, in consultation with the supporting CI organization, prepares a site-specific CI Support Plan (CISP) for each RDT&E site as well as academic and commercial facilities supporting the effort.

- Intelligence organizations provide information concerning technical capabilities that adversaries could use to gain information on specific RDT&E programs or projects.

- Site directors, in coordination with security, intelligence, and CI specialists, should ensure that assigned personnel receive tailored threat briefings.

8.3.2. Protection Approaches

RDT&E conducted within the DoD, as well as by DoD contractors, is covered by the following policies:

- Disclosure of both classified military information and unclassified technical data (DoD Directive 5230.11, "Disclosure of Classified Military Information (CMI) to Foreign Governments and International Organizations;" DoD Directive 5230.24, "Distribution Statements on Technical Documents;" DoD Directive 5230.25, "Withholding of Unclassified Technical Data from Public Disclosure," International Traffic in Arms Regulation, and Export Administration Regulations).

- Control of foreign visitors (DoD Directive 5230.20, "Visits, Assignments, and Exchanges of Foreign Nationals").

- Export control (DoD Directive 2040.2, "International Transfers of Technology, Goods, Services, and Munitions").

For effective protection, the site director (and gaining Program Manager) should integrate these policies into an overall protection strategy, to ensure the identification of DS&TI, the identification of the applicable safeguards, and the effective application of those safeguards. The CISP aids the formulation of an effective protection program at each RDT&E site. Site directors make these policies effective within the RDT&E environment through training and awareness programs.

8.3.2.1. Protection Planning For RDT&E Activities

To conduct effective RTP planning, each RDT&E site director should:

- Review the site RDT&E program periodically and/or whenever there is a significant change in the program.

- Identify information within the RDT&E program that has already been marked for safeguarding (e.g., export control, distribution statement, special handling caveat).

- Identify and prioritize that information as DS&TI.

- Ensure information identified as DS&TI is appropriately marked and disseminated (e.g., export control, distribution statement, special handling caveat).

- Select appropriate countermeasures to protect the DS&TI and identify CI support to be provided.

- Prepare a CISP, with supporting organizations (e.g., CI, security, foreign disclosure, OPSEC, intelligence), tailored to focus protection resources on the identified DS&TI. (The CISP identifies the DS&TI and serves as the "contract" between the individual RDT&E site director and the responsible CI support activity.)

- Communicate the DS&TI to CI, security, foreign disclosure, OPSEC, and intelligence organizations, as appropriate.

8.3.2.2. Assignments, Visits, and Exchanges of Foreign Representatives

The site director should:

- Ensure that assignments, visits, and exchanges of foreign nationals are processed through appropriate channels.

- Ensure that a contact officer has been appointed for each foreign national and is informed of authorized disclosures.

- Establish a process prior to the visit, wherein the relevant technical Point of Contact (POC) and appropriate security and CI personnel communicate the purpose of the visit by the foreign national and the technology and/or program information to be discussed.

- Ensure the process for approving visits by foreign nationals includes dissemination of appropriate disclosure rules and restrictions to RDT&E personnel being visited.

Ensure that foreign nationals are visually identifiable as required by DoD Directive 5230.20.

- Establish a process for archiving information about foreign national visits, including but not limited to, information about the visitor, reason for the visit, information disclosed, and any anomalous event that occurred during the visit.

- Ensure proposed DS&TI releases are reviewed and approved using provision(s) of an Information Exchange Program Agreement (formerly Data Exchange Agreement) prior to release.

- Ensure copies of all international agreements (including MOUs, Information Exchange Program Agreements, and Delegations of Disclosure Letters (DDLs)) relevant to their programs and related systems are maintained and readily accessible to all program personnel as well as supporting CI and security personnel.

8.3.2.3. Export Control

The site director should:

- Establish a process whereby RDT&E personnel determine whether technical data or commodities at RDT&E facilities have been approved for export to foreign countries.
- Establish a focal point at each RDT&E site to determine whether a license for deemed exports is required when a foreign national visits the facility.

8.3.3. Information Assurance

All IT network and systems storing, processing, or transmitting DS&TI should be accredited in accordance with DoDI 5200.40, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)"as described in Chapter 7, Networks and Information Integration.

8.3.4. Counterintelligence Support During Pre-Acquisition

The site director, in consultation with the supporting CI activity, should develop a CISP for each RDT&E site as described in section 8.5.2.

To support the RDT&E site directors, DoD Component CI agencies should:

- Assign CI specialists to support DoD RDT&E activities on or off military installations. The assigned CI specialist(s) will:
    - Provide full-time, tailored, protection support to major DoD RDT&E sites. ("On-call" support will be provided to other DoD RDT&E sites.)
    - Provide, in coordination with the Defense Security Service (DSS), CI support to DoD contractors and academic institutions working with DoD DS&TI.
- Ensure that appropriate security, research management, foreign disclosure, OPSEC, and acquisition program personnel are continuously appraised of foreign intelligence or other threat information relating to their RDT&E site and/or research project.
- Disseminate CI information and products to contractor facilities under DSS cognizance and to other locations and officials that DSS may designate.
- Keep DSS informed of any threat to DS&TI and/or CPI that involve contractors under the cognizance of DSS. Providing classified threat information to contractors will be coordinated with DSS.
- Provide requested threat information to assist defense contractors in developing and updating their Technology Control Plans and protection of DoD DS&TI.

8.4. Acquisition Protection Strategy for Program Managers

8.4.1. Pre-Acquisition Considerations

Program protection planning begins with the Joint Capabilities Integration and Development System as described in CJCS Instruction 3170.01 and in Part 3 of this Chapter. It is integral to the overall acquisition strategy, which is typically developed

prior to formal designation of an acquisition program. The program manager identifies the resources needed (e.g., personnel, fiscal) to accomplish the evaluation and initiate protection as early as possible, but no later than entry into Milestone B.

8.4.2 Acquisition Program Protection - Initiation to Implementation

CPI is the foundation upon which all protection planning for the program is based, and the reason all countermeasures are implemented. Effective program protection planning begins by the program manager reviewing the acquisition program to determine if it contains CPI. If a program manager has not been appointed, the responsible commander/manager or program executive conducts this review. This examination should consider DS&TI previously identified by DoD laboratories, CPI inherited from another program, or CPI that results from non-traditional acquisition techniques (i.e., Advanced Concept Technology Demonstration or flexible technology insertion).

- the program manager (or other official as noted above), with the assistance of a working-level IPT (WIPT), determines the existence of CPI.

- If a program contains CPI, program protection planning is required (see 8.4.5). the program manager (or other official as noted above), with the assistance of a WIPT and/or appropriate support activities, is responsible for developing and implementing a Program Protection Plan (PPP).

- The PPP will be developed, as required, beginning in the Technology Development phase, and will be available to the Milestone Decision Authority at Milestone B and all subsequent milestones during the life cycle of the program. The PPP is revised and updated once every three years, or as required by changes to acquisition program status or the projected threat.

- If there is no CPI associated with the program (either integral to the program or inherited from a supporting program), the program manager so informs the Milestone Decision Authority, Program Executive Officer, or DoD Component Acquisition Executive, as appropriate, and a PPP is not required.

- The next step is for the program manager, through the program management staff, to translate protection requirements into a PPP. This is usually accomplished by a working-level IPT (WIPT) following the process outlined in section 8.4.6. Program protection activities described in sections 8.5.1 to 8.5.6.2 are tailored and performed prior to each milestone to provide the required countermeasures during each acquisition phase.

- After the protection planning foundation is laid, the program proceeds through the milestones and phases of the acquisition process. The program follows an event-based schedule that implements the protection strategy and completes the actions outlined in the PPP.

8.4.3. Programs with Foreign Participation

When a determination is made that any of the following conditions exist, a Technology Assessment/Control Plan (TA/CP) and a Delegation of Disclosure Authority Letter (DDL) should be prepared as annexes to the PPP:

- Foreign participation in system development is possible;

- An allied system will be used;

- The system to be developed is a candidate for foreign sales or direct commercial sales;

- The system will be used in multinational operations; or

- The program will involve cooperative R&D with allied or friendly foreign countries.

Under any of the above conditions, the Foreign Disclosure Officer (FDO) should be involved and informed. With respect to cooperative R&D programs, a Summary Statement of Intent (SSOI), which includes a summarization of the TA/CP, is needed prior to obtaining authority to negotiate the International Agreement that is statutorily required to conduct the program.

If foreign involvement is initiated prior to the appointment of a program manager, the DoD Component generating the capability need should prepare the TA/CP and DDL for Joint Requirements Oversight Council validation and Milestone Decision Authority approval. The program manager, when appointed, should review the requirements for the PPP, TA/CP, DDL, and supporting documentation, and direct the preparation as appropriate.

8.4.4. Risk Management

The overall risk management effort could be a seamless transition between the two following applications, thus allowing a common vernacular for both. Risk management interfaces with acquisition strategy and technology protection. In the current larger scope, risk management has at least two applications.

8.4.4.1. Risk Management in Systems Engineering

In systems engineering, risk management examines all aspects of the program as they relate to each other, from conception to disposal. This risk management approach integrates design (performance) requirements with other Lifecycle issues such as manufacturing, operations, and support.

The program manager should establish a risk management process within systems engineering that includes risk planning, risk assessment (identification and analysis), risk management, and risk monitoring approaches to be integrated and continuously applied throughout the program, including the design process.

This type of risk assessment includes identification and analysis of potential sources of risk, to include cost, schedule, and performance, and is based on such factors as: the technology being used and its relationship to design; manufacturing capabilities; potential industry sources; and test and support processes.

8.4.4.2. Risk Management in Program Protection

In program protection, when viewed within the global context of security, risk management is concerned with technology transfer and is a systematic methodology to

identify, evaluate, rank, and control inadvertent loss of technology. In this respect, it is based on a three-dimensional model: the probability of loss, the severity if lost, and the countermeasure cost to mitigate the loss. As such, risk management is a key element of a program manager's executive decision-making - maintaining awareness of technology alternatives and their potential sensitivity while making trade-off assessments to translate desired capabilities into actionable engineering specifications.

To successfully manage the risk of technology transfer, the program manager should:

- Identify contract vehicles which involve the transfer of sensitive data and technology to partner suppliers;

- Evaluate the risks that unfavorable export of certain technologies could pose for the program; and

- Develop alternatives to mitigate those risks.

8.4.5. Program Protection Planning

When the acquisition program contains CPI, the program manager should initiate a program protection planning process that includes the following steps:

- Identify and set priorities on those operational or design characteristics of the system that result in the system providing unique mission capabilities.

- I dentify and prioritize CPI related to distinctive system characteristics in terms of their importance to the program or to the system being developed. (CPI includes defense technologies and their support systems as defined in DoD Directive 5200.39.)

- Identify specific program locations where CPI is developed, produced, analyzed, tested, maintained, transported, stored, or used in training.

- Identify the foreign collection threat to the program. (MDCI Threat Assessments are discussed in section 8.4.7)

- Identify program vulnerabilities to specific threats at specific times and locations during all phases of the acquisition cycle.

- Identify time- or event-phased RTP countermeasures to be employed by the program manager to reduce, control, or eliminate specific vulnerabilities to the program to ensure a minimum level of protection for CPI.

- Identify anti-tamper (AT) techniques (see section 8.5.3) and system security engineering (SSE) measures (see section 8.5.1) required to protect CPI. Ensure these AT and SSE techniques are included the system's design specifications, subsequent technical drawings, test plans, and other appropriate program documentation.

- Identify elements that require classification and determine the phases at which such classification should occur and the duration of such controls. The resulting program Security Classification Guide is issued by the program Original Classification Authority (OCA).

- Identify protection costs associated with personnel, products, services, equipment, contracts, facilities, or other areas that are part of program protection planning, and countermeasures. These costs are reflected in the program Planning, Programming, and Budgeting Execution System documentation.

- Identify the risks and benefits of developing, producing, or selling the system to a foreign interest, as well as the methods used to protect DS&TI and/or CPI if such an arrangement is authorized. Determine if an export variant is necessary (see section 8.5.1.5).

- Identify contractual actions required to ensure that planned systems security engineering, AT techniques, information assurance, information superiority, classification management and/or RTP countermeasures are appropriately applied by defense contractors at contractor locations (see section 8.5.6). Care should be taken to ensure that measures do not adversely impact the technology of future foreign partners.

- Coordinate with program managers of supporting programs to ensure that measures taken to protect DS&TI and/or CPI are maintained at an equivalent level throughout DoD and its supporting contractors.

After completing the protection planning process, the program manager, assisted by applicable CI and security support activities, ensures implementation of countermeasures to protect the DS&TI and/or CPI at each location and activity identified in the protection planning process. The protection planning process is a dynamic and continuous element, and should remain amenable to appropriate revision.

8.4.5.1. Critical Program Information (CPI)

CPI may include components; engineering, design, or manufacturing processes; technologies; system capabilities and vulnerabilities; and other information that give the system its distinctive operational capability. (Example: A system characteristic might be the small radar cross section. The CPI are those unique program elements that make the small radar cross-section possible.)

When DS&TI are inherited from a technology project and incorporated into an acquisition program, the DS&TI should be identified as program CPI.

8.4.5.1.1. Identifying CPI

To develop the list of CPI, a WIPT should refer to a functional decomposition already performed by the program office, or if necessary, perform a "functional decomposition" of the program or system, as follows:

- Analyze the program or system description and those specific components or attributes that give the system its unique operational capability.

- Analyze each subcomponent until a specific element is associated with each system capability.

- When a specific element is isolated, evaluate its potential as CPI by applying the following questions; an affirmative answer will qualify the item as CPI. If a foreign interest obtained this item or information:
  - Could a method be developed to degrade U.S. system combat effectiveness?
  - Could it compromise the U.S. program or system capabilities?
  - Would it shorten the expected combat-effective life of the system or significantly alter program direction?
  - Would additional RDT&E resources be required to develop a new generation of the U.S. system that was compromised?
  - Would it compromise the U.S. economic or technological advantage?
  - Would it threaten U.S. National Security?
- In addition to the elements organic to the system, the program manager should consider any engineering process, fabrication technique, diagnostic equipment, simulator, or other support equipment associated with the system for its identification as a possible CPI. Special emphasis should be placed on any process that is unique to the system being developed. The program manager and program engineer should evaluate each area and identify any activity distinctive to the U.S. industrial and technological base that limits the ability of a foreign interest to reproduce or counter the system.

8.4.5.1.2. Refining CPI

Once all system CPI has been identified, additional refinement may be necessary. Key considerations in this refinement follow:

Describe CPI in terms understandable by those not in the scientific or engineering field (e.g., use terms from the Militarily Critical Technology List (MCTL) or National Disclosure Policy). The fact that a particular technology is on a technology control list does not mean that particular technology is a CPI.

- Provide specific criteria for determining whether CPI has been compromised.
- Indicate any CPI related to a treaty-limited item.
- Indicate if this CPI is being or may be used by any other acquisition program or system.
- Prioritize CPI to ensure that the most important information is emphasized during protection cost analysis. That process addresses the following three questions:
  - What is the threat to U.S. National Security?
  - What is the extent to which the CPI could benefit a foreign interest?
  - How difficult is it for a foreign interest to exploit the information?

8.4.5.1.3. Inherited DS&TI and CPI

The program manager should identify and prioritize DS&TI and/or CPI for any component, subsystem, technology demonstrator, or other independent research program that will be incorporated into the program manager's program. The using program manager should ensure such CPI is addressed in the subsystem PPP. Conversely, the program manager of a subsystem program with CPI should ensure that their CPI is included in the major program PPP.

- The program manager of a new system will ensure that CPI shared or gained from a subsystem is protected in the new system to at least the same level of protection afforded in the subsystem program.

- A program manager of a system that incorporates a subsystem not reviewed to identify CPI should request the subsystem program office to review their program and supply the resulting information and/or documentation.

- When supporting activities defined as acquisition programs have not developed a PPP to protect their CPI, the program manager incorporating the technology in question should request the subsystem program manager to develop and provide an approved PPP.

8.4.5.2. Collaboration

The program manager is responsible for developing, approving, and implementing a PPP, normally through a WIPT. the program manager may establish a research and technology protection WIPT or include the appropriate personnel on an existing WIPT to assist in preparing the PPP and its supporting documentation.

CI and security support activities and program protection staff elements should assist the program manager in identifying CPI.

The following personnel or organizational representatives are normally represented in the research and technology protection (RTP)WIPT:

- Program office engineering and/or technical staff

- System user representative

- Maintenance and logistics representative

- Organizational or command security manager

- Counterintelligence

- Intelligence

- Operations security

- Foreign disclosure

- Base, installation, or post physical security staff

- Organization RTP staff representative

- Information Assurance Manager and/or information systems security manager

The program manager should ensure close coordination and cooperation between the security, foreign disclosure, intelligence, operations security, CI, physical security, and RTP offices and the program office staff during development of a PPP.

8.4.6. Program Protection Plan (PPP)

The PPP is the program manager's single source document used to coordinate and integrate all protection efforts designed to deny access to CPI to anyone not authorized or not having a need-to-know and prevent inadvertent disclosure of leading edge technology to foreign interests. If there is to be foreign involvement in any aspect of the program, or foreign access to the system or its related information, the PPP will contain provisions to deny inadvertent or unauthorized access.

The program manager establishes and approves the PPP for an acquisition program as soon as practicable after validation of the Initial Capabilities Document and the determination that CPI exists.

Preparation and implementation of a PPP is based on effective application of systematic risk management methodology, not risk avoidance. Costs associated with protecting CPI are balanced between protection costs and potential impact if compromised. In some cases, residual risks may have to be assumed by the program; such decisions rest with the Milestone Decision Authority, based upon the recommendation by the program manager.

The following guidance describes the process used to prepare a PPP when one is required:

- Any program, product, technology demonstrator, or other item developed as part of a separate acquisition process, and used as a component, subsystem, or modification of another program, should publish a PPP.

- Effectiveness of the PPP is highly dependent upon the quality and currency of information available to the program office.

    o Coordination between the program office and supporting CI and security activities is critical to ensure that any changes in the system CPI, threat, or environmental conditions are communicated to the proper organizations.

    o Intelligence and CI organizations supporting the program protection effort should provide timely notification to the program manager of any information on adverse foreign interests targeting their CPI without waiting for a periodic production request.

The PPP is classified according to content.

The degree of detail in the PPP should be limited to information essential to plan and program the protection of CPI, and to provide an executable plan for implementing the associated countermeasures throughout the pre-acquisition and acquisition phases. While there is no specific format for PPPs, they normally include the following:

- System and program description;

- All program and support points of contact (POCs);

- A prioritized list of program CPI;

- Multidiscipline Counterintelligence (MDCI) threat assessment to CPI;

- Vulnerabilities of CPI;

All RTP countermeasures (e.g., AT techniques, SSE) and Militarily Critical Technology List (MCTL) citations for applicable DS&TI or CPI;

- All RTP associated costs, by Fiscal Year, to include PPP development and execution;

- CI support plan (CISP);

- Current Security Classification Guide (SCG);

- Foreign disclosure, direct commercial sales, co-production, import, export license or other export authorization requirements, and/or TA/CP; and

- Delegation of Disclosure Authority Letter, if appropriate.

The following sections provide specific guidance related to some PPP topics listed above.

8.4.6.1. System and Program Descriptions

System Description. Since most acquisition programs combine existing, proven technology, as well as information with state-of-the-art technology, the system description included in a PPP provides the reviewer with a clear indication of the capabilities and limitations of the system being acquired, including simulators and other supporting equipment. The purpose of the system description is to set the stage for identifying CPI. The system description should be based on the approved Initial Capabilities Document and Capability Development Document and include:

- Anticipated employment of the system within the battle space, along with the strategic, operational, or tactical impact of the system; and

- Specific characteristics that distinguish the system from existing systems, other systems under development, or that provide the system with unique operational or performance capability.

Program Description. This section is a short summary of the organization and structure of the office responsible for developing and fielding the acquisition system. Early in the acquisition process, that information may be somewhat limited. Detail should be added as participants in the program are identified and as their role in program protection activities becomes known. The program description should briefly describe the following:

- The program management chain of command, including the Program Executive Officer, DoD Component Acquisition Executive, and/or Milestone Decision Authority for the program and supporting programs;

- The locations, points of contact (POCs), and telephone numbers of prime contractors, sub-contractors, vendors, DoD sites, Federal agencies, Government Owned - Contractor Operated and DoD RDT&E activities and/or facilities that will handle, store, or analyze CPI-related material;

- DoD Component and/or other DoD organization partners that are equity holders; and

- Likelihood that these technologies or this program will transition to another DoD Component / DoD organization in the future.

8.4.6.2. Foreign Collection Threat

Foreign collection threat assessment used by the program office in planning protection for the CPI should be based upon a National-level intelligence estimate known as a "MDCI Threat Assessment"

- The MDCI threat assessment is prepared and produced as a stand-alone document by the applicable DoD CI analysis center (see section 8.4.7);

- The MDCI threat assessment should not be confused with a System Threat Assessment (STA); the MDCI threat assessment identifies foreign interests having a collection requirement and a capability to gather information on the U.S. system being developed;

- Sudden changes in the operational threat should be reviewed as they occur to determine if the changes are due to successful foreign intelligence collection;

- The program manager and WIPT should compare results of the MDCI threat assessment with the CPI and vulnerabilities to determine the level of risk to the program; and

- The WIPT should integrate environmental factors and arms control-related issues that might reduce the ability of foreign interests to collect information at a given location in the MDCI threat assessment, where applicable.

A threat exists when:

- A foreign interest has a confirmed or assessed requirement for acquiring specific classified or sensitive defense information or proprietary or intellectual property information;

- A foreign interest has the capability to acquire such information; and/or

- The acquisition of such information by the foreign interest would be detrimental to U.S. interests.

Confirmed or assessed identification of foreign collection requirements provide indicators of probable sources or methods employed to satisfy a collection requirement.

CI and security support activities assist the program office in preparing collection requirements and production requests to applicable DoD Component intelligence or CI analysis centers.

- CI and security support activities should submit the request to the intelligence center that normally supports the program manager; and

- An informational copy is sent to the intelligence analysis center of any other DoD Component involved in the program to facilitate a single and unified position on the collection threat. CIFA is also provided a copy.

8.4.6.3. Vulnerabilities

Vulnerability is the susceptibility to compromise of a program to a threat in a given environment. Vulnerabilities to the program's CPI are based upon one or more of the following:

- How CPI is stored, maintained, or transmitted (e.g., electronic media, blueprints, training materials, facsimile, modem);

- How CPI is used during the acquisition program (e.g., bench testing, field testing);

- Emanations, exploitable signals, or signatures (electronic or acoustic) that are generated or revealed by the CPI (e.g., telemetry, acoustic energy, radiant energy);

- Where CPI is located (e.g., program office, test site, contractor, academia, vendor);

- Types of OPSEC indicators or observables that are generated by program or system functions, actions, and operations involving CPI;

- Conferences, symposia, or foreign travel that the program manager and staff members participate in or plan to be involved in;

- The level of human intelligence or insider threat that is evident or projected at the program management location or other locations where CPI will be located;

- Foreign disclosures that are planned, proposed, or staffed for release;

- Degree of foreign participation that is currently pursued or being planned for the program or locations where CPI will be located;

The program manager should prioritize identified vulnerabilities;

- Prioritization is based upon the consequences if CPI is lost or compromised, and the level of difficulty for a foreign interest to exploit the information; and

- Factors to be considered include the adverse impact on the combat effectiveness of the system, the effect on the combat-effective lifetime, and the cost associated with any modifications required to compensate for the loss.

8.4.6.4. RTP Countermeasures

These are measures employed to eliminate or reduce the vulnerability of CPI to loss or compromise, and include any method (e.g., AT techniques, information assurance) that effectively negates a foreign interest capability to exploit CPI vulnerability.

RTP countermeasures are developed to eliminate vulnerabilities associated with an identified threat to CPI based upon the authoritative, current, and projected threat information in the MDCI threat assessment. RTP countermeasures will:

- Be applied in a time- or event-phased manner (e.g., for certain periods of time, until milestones within program development).

- Be implemented until they are no longer required. They are terminated or reduced as soon as practicable after the threat, CPI, or environmental changes lead to a reduction or elimination of the vulnerabilities or a negation of the threat. For example, arms control countermeasures might be implemented only while the facility is vulnerable to a mandated arms control treaty inspection or an over flight by foreign inspectors.

- Address DoD Information Technology Security Certification and Accreditation Process (DITSCAP) compliance for all information technology systems and/or networks.

The program manager should establish a countermeasures program based upon threat, risk management, OPSEC methodology, and vulnerability assessments. The program manager should determine the costs associated with countermeasure application or implementation, and compare them to the risk associated with loss or compromise of the CPI. Whenever countermeasures to reduce, control, or eliminate a CPI vulnerability will not be developed, the program manager should provide a justification for that decision in the countermeasures section of the PPP.

If the acquisition program does not have an assigned or contracted security organization, applicable CI and security support activities should assist the program office in developing a draft countermeasures concept based upon the program manager's guidance. The program manager should designate the element of the program office responsible for publishing the PPP.

Additional RTP countermeasure considerations include the following:

- Countermeasures recommended to eliminate or reduce vulnerabilities associated with CPI at government and contractor facilities, may not be waived while the affected facilities are vulnerable to arms control treaty inspections or over flights by foreign interests.

- The requirement for contractor compliance with the government-approved PPP is included in the government solicitation and the resulting contract(s) (see section 8.4.9).

- Training in protection of research and technology information and security awareness is integral to the countermeasures effort.

    o Following approval of the PPP, the program manager should implement a training program to inform all program members of the requirements in the PPP and, if applicable, the requirements and guidelines established in the DDL, which is a U.S.-only document.
    o Emphasis is placed on encrypting the transmission of electronic messages, facsimile transmissions, and telephone transmissions relating to CPI,

underpinning technologies, and other CUI related to programs containing DS&TI or CPI. These transmissions should be via Federal Information Processing Standard 140-2 compliant encryption.

- Countermeasures are dynamic. As the threat, CPI, or environment changes, the countermeasures may also change. The program manager should update the PPP as system vulnerabilities change, and thus reduce the cost of and the administrative burden on their program.

8.4.6.5. Security Classification Guide (SCG)

When necessary, the program manager must develop a SCG in accordance with DoD 5200.1-R. The SCG addresses each CPI, as well as other relevant information requiring protection, including export-controlled information and sensitive but unclassified information.

All controlled unclassified information, information identified as "FOUO" as defined in DoD 5400.7-R, or information with other approved markings that require dissemination controls (e.g., DoD Directive 5230.24 and DoD Directive 5230.25, is exempt from mandatory disclosure under the Freedom of Information Act and will be identified in the SCG.

The SCG will be reviewed, and amended when necessary, as part of each milestone review or as otherwise required by DoD 5200.1-R

8.4.6.6. Protection Costs

Cost data associated with countermeasures and other RTP efforts are compiled by the RTP WIPT, tabulated by acquisition phase, and included in the PPP. Cost accounting only addresses the costs specific to the implementation of the PPP and excludes projected costs for operating with classified information. (See section 8.4.9.5.)

Costs should be displayed by security discipline (e.g., physical security, personnel security, industrial security) and category (e.g., equipment, services, personnel). Cost data for each phase should be as specific as possible. Additionally, actual annual costs for the previous phase should be compiled and compared with the projected annual cost for the current acquisition phase. Significant deltas showing differences between projected and actual cost data should be explained. This information is used for justifications required by the Planning, Programming, and Budget System.

The Acquisition Program Baseline includes costs related to PPP implementation.

8.4.7. Multidiscipline CI (MDCI) Threat Assessment

When an acquisition program containing CPI is initiated, the program manager should request a MDCI threat assessment from the servicing CI organization. The MDCI threat focuses on how the opposition sees the program and on how to counter the opposition's collection efforts. The MDCI analyst, in addition to having an in-depth understanding and expertise on foreign intelligence collection capabilities, must have a good working knowledge of the U.S. program. Therefore, CI organizations need information that

describes the CPI and its projected use to determine the foreign collection threat to an acquisition program.

The MDCI threat assessment will provide the program manager with an evaluation of foreign collection threats to specific program or project technologies, the impact if that technology is compromised, and the identification of related foreign technologies that could impact program or project success. The MDCI threat assessment is updated every two years throughout the acquisition process. Changes are briefed to the program or project manager within 60 days.

When gathering information to meet the needs described in this Chapter, intelligence and CI organizations must comply with DoD Directive 5240.1 and DoD 5240.1-R. Information gathered by non-intelligence community entities must comply with DoD Directive 5200.27.

8.4.7.1. Threat Analysis Request

The program manager's request to the CI organization for a threat assessment normally contains the following information and is classified as appropriate:

- Program office, designator, and address;
- program manager's name and telephone number;
- POC's name, address, and telephone number;
- Supporting or supported programs' or projects' names and locations;
- Operational employment role, if any;
- List of CPI;
- Relationship to key technologies or other controlled technology lists of the Departments of Defense, Commerce, and/or State;
- CPI technical description, including distinguishing characteristics (e.g., emissions; sight or sensor sensitivities) and methods of CPI transmittal, usage, storage, and testing;
- Use of foreign equipment or technology during testing (if known);
- Anticipated foreign involvement in the development, testing, or production of the U.S. system;
- Contractor names, locations, POCs, and telephone numbers, as well as the identification of each CPI used at each location; and
- Reports of known or suspected compromise of CPI.

8.4.7.2. Preliminary MDCI Threat Assessment

After the request is submitted, the Component CI organization provides a preliminary MDCI threat assessment to the program manager within 90 days. A preliminary assessment is more generic and less detailed than the final assessment. It is limited in use since it only provides an indication of which countries have the capability to collect intelligence on the U.S. system or technology as well as the possible interest and/or

intention to collect it. The preliminary MDCI assessment may serve as the basis for the draft PPP.

8.4.7.3. Final MDCI Threat Assessment

The program manager submits the draft PPP for approval only after the final MDCI threat assessment has been received from the applicable DoD Component CI and/or intelligence support activity. Normally, the MDCI threat assessment is returned to the requesting program office within 180 days of the CI and/or intelligence organization receiving the request.

The MDCI threat assessment answers the following questions about CPI:

- Which foreign interests might be targeting the CPI and why?

- What capabilities does each foreign interest have to collect information on the CPI at each location identified by the program office?

- Does evidence exist to indicate that a program CPI has been targeted?

- Has any CPI been compromised?

8.4.8   Technology Assessment / Control Plan (TA/CP)

8.4.8.1 General

The policy on TA/CP is in DoD Directive 5530.3

Prior to formal negotiation, the program manager prepares a TA/CP, or similar document, as part of the PPP for all acquisition programs with international involvement. The TA/CP is included in the PPP when it is determined that there is likely to be foreign involvement in the development program or when there will be foreign access to the resulting system or related DS&TI or CPI, by virtue of foreign sales, co-production, follow-on support, exchange program, training, or multinational exercises or operations. Much of the information required for the preparation of the TA/CP can be obtained from the Initial Capabilities Document/Capability Development Document, the Analysis of Alternatives, the acquisition strategy, and the justification and supporting information used in preparing those documents.

8.4.8.2. Purpose

The program manager uses the TA/CP to do the following:

- Assess the feasibility of U.S. participation in joint programs from a foreign disclosure and technical security perspective.

- Prepare guidance for negotiating the transfer of classified information and critical technologies involved in international agreements.

- Identify security arrangements for international programs.

- Provide a basis for the DDL that contains specific guidance on proposed disclosures.

- Support the acquisition decision review process.

- Support decisions on foreign sales, co-production, or licensed production, commercial sales of the system, or international cooperative agreements involving U.S. technology or processes.

- Support decisions on the extent and timing of foreign involvement in the program, foreign sales, and access to program information by foreign interests.

W hen it is likely there will be foreign involvement in the program, or foreign access to the resulting system or related information, it is advantageous for the program manager to prepare the TA/CP after completing the identification of DS&TI, CPI, and security classification guidance. The TA/CP analysis often assists in developing vulnerabilities and proposed RTP countermeasures. Policies governing the foreign disclosure of intelligence information are in Director of Central Intelligence Directives (DCIDs) 1/7 and 5/6, information security products and information in National Security Telecommunications and Information Systems Security (NSTISS) Policy Number 8, and nuclear information governed by the Atomic Energy Act. These documents must be consulted when these types of information are involved in an acquisition program.

8.4.8.3. Content

The TA/CP is composed of four sections: the "Program Concept"; the "Nature and Scope of the Effort and the Objectives"; the "Technology Assessment"; and the "Control Plan." Those TA/CP subsections are the basis for preparing the DDL.

Program Concept . This section requires a concise description of the purpose of the acquisition program. It should describe, in the fewest words possible, the purpose of the system and the system threat or the military or technical requirements that created the need for the system. The description must be consistent with the PPP.

Nature and Scope of Effort and the Objectives . This section briefly explains the operational and technical objectives of the program (e.g., co-production, cooperative research and development) and discusses any foreign participation or involvement. If foreign participation or involvement or the release of information to support potential foreign sales is considered likely, the phasing and disclosures at each phase should be described briefly. The milestones, foreign entities expressing interest, and summary of expected benefits to the U.S. should also be covered. The POC for all aspects of the TA/CP must be identified, including address, telephone numbers, and facsimile numbers.

Technology Assessment . The third section is the most important part of the TA/CP. It analyzes the technology involved in the program, its value, and the consequences of its compromise. It should provide conclusions regarding the need for protective security measures and the advantages and disadvantages of any foreign participation in the program, in whole or in part, and should describe foreign sales. The assessment should be specific concerning the phased release of classified and unclassified information that supports potential foreign involvement and foreign sales. Since preparation of this section requires a joint effort involving program management, security, intelligence, and foreign disclosure personnel, it may be a task for the RTP WIPT.

When the TA/CP is prepared in the early stages of program protection planning, emphasis should be placed on describing the value of the technology and systems in terms of military capability, the economic competitiveness of the U.S. industrial base and technology, susceptibility to compromise, foreign availability, and likely damage in the event of compromise.

This assessment should result in a conclusion on whether a cooperative program, co-production, or foreign sale will result in clearly defined operational or technological benefits to the United States, and whether these benefits would outweigh any damage that might occur if there should be a compromise or unauthorized transfer. Specific reasons must be provided.

This assessment should identify and explain any critical capability, information, or technology that must be protected. It may reveal that an adjustment to program phasing is necessary so critical information is released only when absolutely necessary. It should identify any CPI that may not be released due to the impact on the system's combat effectiveness. Additionally, it will identify the need for special security requirements such as a program-specific security plan to govern international involvement. The assessment should also evaluate the risk of compromise, based on the capability and intent of foreign participants or purchasers to protect the information, and the susceptibility of the system to compromise if not protected.

Finally, the assessment should discuss any known foreign availability of the information, system, or technology involved; previous release of the same or similar information, system, or technology to other countries; and, when foreign involvement or sales are recommended, its release to other participants.

Control Plan . The fourth section, together with the technology assessment, provides the basis for guidance on negotiating technical and security aspects of the program, and development of disclosure guidelines for subsequent sales and foreign participation in the program.

The Control Plan should describe actions that are to be taken to protect U.S. interests when foreign involvement or sales are anticipated. Those actions should be specific and address specific risks, if any, as discussed in the technology assessment. Actions might include withholding certain information, stringent phasing of releases, or development of special security requirements.

The plan should also identify any design or engineering changes that may be necessary or desirable to ensure the protection of CPI. The plan should describe how security provisions of an agreement and/or applicable regulations are to be applied to the specific program, agreement, or sale.

In preparation of the Control Plan, special consideration should be given to the export restrictions on sensitive technologies and materials amplified in DoD Instruction S-5230.28 and the National Disclosure Policy Committee's Policy Statement on "Foreign Release of Low Observable and Counter Low Observable Information and Capabilities (U)".

Delegation of Disclosure Authority Letter (DDL). The program manager must prepare a DDL as part of a recommendation for foreign involvement, disclosure of the program to

foreign interests, request for authority to conclude an international agreement, or a decision to authorize foreign sales. NOTE: The DDL is not releasable to Foreign Nationals.

The DDL should provide detailed guidance on releasability of all elements of the system, to include its technology and associated information. The Security Classification Guide (SCG) will be consulted during the preparation of the DDL to establish its classification.

The program manager develops the DDL in accordance with DoD Directive 5230.11 enclosure 4. The applicable designated disclosure authority should agree with its content. The DDL is provided to the Milestone Decision Authority and the Office of the USD(P) for approval at each milestone. Until the DDL has been approved by the originating activity's designated disclosure authority, the Milestone Decision Authority, and the Office of the USD(P), there should be no promise to release, nor should there be actual release of, sensitive information or technology.

8.4.9. Contracting and Resources

Program protection planning may be outsourced and included in a contract. That contract activity may include initial program and system evaluation as well as program protection planning that leads to specific RTP countermeasures. Early planning is necessary to ensure that funds are programmed and budgeted to provide timely required contract support.

Program protection activities should begin prior to contract award. Delaying the process may result in safeguards being difficult to accomplish or being omitted from contracts. The program's underpinning DS&TI, and inherited or determined CPI, should be factored into the program's overall acquisition strategy. The program manager is responsible for this planning and should prepare a budget for all security costs within the Planning, Programming, Budgeting, and Execution (PPBE) process and the program's Acquisition Program Baseline. It is more cost effective for security to be "baked in" early rather than "bolted on" later.

8.4.9.1. Early Coordination

As discussed in section 8.4.2, RTP is a subject for early coordination by the program manager's staff and contracting personnel to ensure contractual documents contain essential protection requirements. Early coordination is fundamental for having adequate coverage in contractual documents and to thus avoid additional and unnecessary costs due to late application of RTP requirements. The expected range of protection requirements and projected resources required should be estimated to ensure research and acquisition planning documents address RTP. RTP is also a subject for early coordination by FDOs.

8.4.9.2. Pre-Contract Award

The pre-award phase includes pre-solicitation, solicitation, source selection evaluation, and other pre-award activities.

Acquisition organizations generally have local instructions and related checklists to aid the program management staff in completing the actions necessary to arrive at a legal and

successful contract award. Such instructions and checklists should be written and reviewed to ensure they address program protection activities and requirements.

The program manager should define program protection requirements early enough to be included in the draft request for proposal (RFP).

- The initial program management staff, with the assistance of the program protection POC, provides the responsible contracting office with information describing the nature and extent of program protection requirements that apply to the contemplated contract and estimates for the resources necessary to contractually execute the program. (See the information listed in subsection 8.4.6.)

- The PM includes a program protection section in the RFP and should ensure that the appropriate Federal Acquisition Regulation (FAR) and/or Defense Federal Acquisition Regulation Supplement (DFARS) clauses have been activated for RTP (e.g., DFARS 242.402).

Once the proposals are received in response to the RFP, they will be evaluated using specified source selection criteria. The resulting evaluation should address the proposed ways of satisfying program protection requirements. The evaluation should also consider the cost to execute each proposed approach to satisfy the contractor portion of the PPP. An RTP specialist should be available to assist in the source selection process when proposals are required to address program protection requirements.

Approaches in the selected contractor's proposal documents should be incorporated into the contract. Action should be taken to ensure RTP provisions in the proposal are fully implemented by the prime contract.

The program manager should require the contractors to coordinate with the program office staff and CI support staff, all proposals to market or otherwise obtain a commercial export license to sell portions of the system being acquired or like systems to foreign countries. The PM should formalize this requirement in all Statements of Work for acquisition systems. A lack of coordination by the contractors may result in inadvertent transfer of critical military technology to unauthorized foreign nationals.

8.4.9.3. Post Contract Award

It is not unusual for contract modifications to be made reflecting fiscal or other program changes. As with pre-award actions, the program manager should ensure that the program office RTP representative works with the program management staff and the contracting officer if RTP changes are required.

A primary post award activity is "baselinin" the contract. RTP actions are addressed in this activity and, if applicable, identified as a reportable item in the baseline. When used, the contractor program protection implementation plan (PPIP) forms a principal source for the contract RTP baseline.

The contracting officer representative (COR) is formally identified during post award activities and becomes the focal point, along with the program manager, for administering contract requirements, including RTP. The COR and the program manager

need to understand how RTP is important to successful achievement of protecting the program cost, schedule, and performance objectives. The COR should discuss the security requirements with the FDO.

8.4.9.4. Contractor Performance Monitoring

The COR, along with the program manager and contracting officer (CO), are key to ensuring that RTP requirements are accomplished, particularly if there are any modifications to the contract. The RTP POC should monitor performance and schedule of RTP activities. As part of the program manager staff, the RTP POC works through the program manager, COR, and CO in accomplishing RTP goals. Any proposed contract modifications regarding foreign involvement should also be discussed with the FDO.

Planning for performance monitoring begins with RFP activities, pre-award issues, and continues with the contract baselining and any necessary re-baselining.

The contract baseline, once documented, will be the prime contractor performance measurement tool. That baseline is compared with periodic performance reports that address work accomplished as well as costs incurred and related task funding. When the work breakdown structure is developed, any RTP action identified in the statement of work, preliminary acquisition planning activities, or the RFP, is identified as a "reportable item"

8.4.9.5. Contractor Costs

To properly support contract activities, RTP costs are identified as part of the initial program definition and structuring. Those cost estimates are then used in the early contract development process, starting with drafting of the RFP.

Cost estimates are identified by category (i.e., personnel, products, services, equipment) to include any information systems requirements. Within each category of RTP costs, the items are further identified by security discipline.

Costs for implementing industrial security are included in the overhead portion of contractor costs. DoD security countermeasures are typically included in level-of-effort costs for DoD agencies. These costs should not be included in the PPP since they are not additive costs to the acquisition program. The baseline for standard security actions is determined before identifying program-specific RTP costs.

RTP costs for implementing foreign disclosure and/or national disclosure policies are also identified by the categories listed in the paragraphs above.

8.4.9.6. Providing Documentation to Contractors

The program manager, in coordination with the RTP POC and the contracting officer, determines when prime contractors, and subcontractors supporting the RTP effort, need access to CPI documentation. If a foreign contractor is involved, the Foreign Disclosure Officer (FDO) must participate in the coordination.

When a contractor is to be granted access to classified information, sensitive information, controlled unclassified information, For Official Use Only information, export-controlled data, or unclassified technical data, the contract will provide authorization for access to

contractor facilities by the responsible government industrial security office (DSS or the DoD Component-cognizant security authority). That authorization is necessary to permit surveys, inspections, advice or assistance visits, or inquiries, which are necessary to ensure protection of sensitive information and implementation of RTP activities at prime, subcontractor, and/or vendor facilities.

Whenever possible, threat information (i.e., MDCI threat assessment) is shared with the cognizant contractor Facility Security Officer to ensure their understanding of the threat.

8.4.9.7. Support from Cognizant Government Industrial Security Offices

The contract DD Form 254, "DoD Contract Security Classification Specification," should specifically identify RTP assessments and reviews to be conducted by the responsible government industrial security office (e.g., DSS). The program manager should complete the DD 254 to reflect RTP protection measures and requirements. A copy of the DD 254 should be provided to the cognizant government security office (i.e., the appropriate DSS field office) so they may assist in RTP protection efforts. Organizations responsible for RTP reviews should:

- Conduct or participate in reviews and assistance visits at contractor facilities and contractor activities at government facilities. Reviews at contractor facilities in the United States assess compliance with contractually-imposed RTP measures, when contract provisions authorize such reviews and visits.

- Disseminate evaluation reports to appropriate acquisition program officials (e.g., Program Executive Officers, program managers, user organization officials). Unless specifically prohibited, the program manager provides reports to appropriate contractor personnel.

8.4.10. RTP Costing and Budgeting

Ultimately, the success of an acquisition program will depend on protecting the research and technology upon which the acquisition is based. RTP requirements should be incorporated into initial program funding and subsequent budget submissions to ensure adequate resources are committed at program initiation.

When RTP professionals are part of the program costing and budgeting processes, RTP requirements can be addressed during programming and budgeting cycles.

8.4.10.1. RTP Costing

Program resource managers are responsible for developing a Work Breakdown Structure and Cost Analysis Requirements Description as part of the overall costing process. The Cost Analysis Requirements Description is developed in concert with the Work Breakdown Structure and serves as the costing portion of the Work Breakdown Structure. Costs for material, personnel/labor, training, etc., are incorporated into a requirements document to define overall RTP costs. Security, counterintelligence, and intelligence professionals should be integrated into the program costing process at the earliest opportunity.

A separate Work Breakdown Structure category provides managers with visibility into RTP costs and actual funding available to support the RTP effort. A separate Work Breakdown Structure category is recommended for RTP requirements such as anti-tamper, system security engineering, information assurance, and the program protection implementation plan (PPIP).

8.4.10.2. RTP Budgeting

Once RTP cost requirements are properly estimated and documented, the next step in the process is their submission and validation as part of the program budgeting process. All RTP costing requirements are coordinated with the program resource manager who prepares budget submissions to the program manager.

Often, a validation board is assembled to review program costing requirements. This board validates the cost (verifies the methodology used to project the costs) and prioritizes program cost requirements. When RTP cost proposals are submitted, RTP professionals should be present to support these proposals to the validation board. RTP professionals should serve as advisors to the program manager for RTP costs coming from other organizations or from contractors.

Once a program budget is approved and the RTP requirement funded, establishing a separate RTP funding line item could be useful in tracking funds that are distributed to support RTP requirements.

RTP POCs who manage funding and/or the implementation of the PPIP are required to annually update their funding requirements and contribute to the overall program budget submission process. RTP costs will be validated each year.

8.4.11. Execution of the PPP

The program manager has the primary responsibility for PPP execution. Specific functions and actions may also be assigned to supporting security, CI, and intelligence organizations, as well as supporting acquisition organizations and defense contractors. Proper PPP execution depends on allocation of resources for planned RTP countermeasures and communication of the RTP countermeasures plan to applicable contractors, as well as to acquisition, security, CI, and intelligence activities supporting the program.

8.4.11.1. Distribution of the PPP

Once the PPP is approved, the program manager ensures all activities that are assigned RTP actions in the PPP receive a copy of the approved plan or those portions pertaining to their tasks. Organizations that should be considered for PPP distribution include the following:

- Program contractors having CPI under their control.

- Responsible government industrial security offices (i.e., DSS offices supporting the program at contractor sites covered by the PPP and/or the PPIP).

- DoD test ranges and centers applying CPI countermeasures.

- CI activities supporting program sites having CPI countermeasures applied.

If the program manager decides to limit distribution of the entire PPP, then, as a minimum, the CPI and RTP countermeasures portions should be distributed to the appropriate organizations.

8.4.11.2. Assessment of PPP Effectiveness

The program manager, assisted by security and CI activities, assesses PPP effectiveness, and the RTP countermeasures prescribed therein, as part of the normal program review process. Such assessments are planned considering the overall program schedule, the time-phased arrival or development of CPI at specific locations, and the schedule to revise the PPP.

8.5   Specialized Protection Processes

8.5.1   System Security Engineering

8.5.1.1 General

If the program manager decides to use system security engineering (SSE) it can be the vehicle for integrating RTP into the systems engineering process. Systems engineering activities prevent and/or delay exploitation of DS&TI and/or CPI in U.S. defense systems and may include Anti-Tamper (AT) activities (see section 8.5.3). The benefit of SSE is derived after acquisition is complete by mitigation of threats against the system during deployment, operations, and support. SSE may also address the possible capture of the system by the enemy during combat or hostile actions.

8.5.1.2. System Security Engineering Planning

The program manager's System Engineering Plan (SEP) is the top-level management document used to describe the required systems engineering tasks. The System Security Management Plan (SSMP) is a detailed plan outlining how the SSE manager (SSEM) and the contractors will implement SSE, and may be part of the SEP.

The SSMP, prepared by the program manager, establishes guidance for the following tasks:

- Analysis of security design and engineering vulnerabilities; and

- Development of recommendations for system changes, to eliminate or mitigate vulnerabilities through engineering and design, any characteristics that could result in the deployment of systems with operational security deficiencies.

The SSMP is applicable to the acquisition of developmentalor existing systems or equipment.

MIL-HDBK-1785 establishes the formats, contents, and procedures for the SSMP. Data Item Description (DID), DI-MISC-80839, SSMP, is applicable.

A System Security Engineering Working Group (SSEWG) defines and identifies all SSE aspects of the system, develops SSE architecture, reviews the implementation of the

architecture, and participates in design validation. The SSEWG is formed as early in the acquisition process as possible, but not later than the Technology Development phase of the acquisition. The SSEWG is comprised of acquisition program office personnel; supporting CI, intelligence, and security personnel; system user representatives; and other concerned parties. The SSEWG provides recommendations to the program manager.

8.5.1.3. System Security Engineering Process

SSE supports the development of programs and design-to-specifications providing Lifecycle protection for critical defense resources. Activities planned to satisfy SSE program objectives are described in the SSMP.

SSE secures the initial investment by "designing-in" necessary countermeasures and "engineering-out" vulnerabilities, and thus results in saving time and resources over the long term. During the system design phase, SSE should identify, evaluate, and eliminate (or contain) known or potential system vulnerabilities from deployment through demilitarization.

The SSE process defines the procedures for contracting for an SSE effort and an SSMP. Implementation requires contractors to identify operational vulnerabilities and to take action to eliminate or minimize associated risks.

Contract Data Item Descriptions (DIDs) and Contract Data Requirements Lists (CDRLs) may be tailored to the acquisition program in order to obtain contractor-produced plans or studies that satisfy specific program needs.

8.5.1.4. Military Handbook 1785

MIL-HDBK-1785 contains procedures for contracting an SSE effort and an SSMP. The format and contents are outlined in the appropriate Data Item Descriptions (DIDs) listed in MIL-HDBK-1785.

The proponent for the handbook is Commander, Naval Air Systems Command, ATTN: AIR-7.4.4., 22514 McCoy Road, Unit 10, Patuxent River, MD 20670-1457.

8.5.1.5. Security Engineering for International Programs

SSE should include an assessment of security criteria that sets limits for international cooperative programs, direct commercial sales, and/or foreign military sales (FMS) cases. From this assessment, engineering and software alternatives (e.g., export variants, AT provisions) should be identified that would permit such transactions.

8.5.2. Counterintelligence Support Plan

The CISP defines specific CI support to be provided to the RDT&E facility or acquisition program and provides the servicing CI personnel with information about the facility or program being supported.

- A tailored CISP is developed for every DoD RDT&E activity and for each DoD acquisition program with identified CPI;

- RDT&E site directors, security managers, and supporting CI organizations are responsible for developing a CISP for each RDT&E facility;

- Program managers and their supporting security and CI organizations are responsible for developing a CISP for each acquisition program with CPI. The CPI will be prioritized and listed in the CISP;

- The CISP is signed by local CI and site management personnel, the program manager, and the local DSS representative, as appropriate. The CISP will specify which of the CI services will be conducted in support of the facility or program, and will provide the CI personnel with information about the program or facility to help focus the CI activities. A copy of the signed plan is provided to the DoD Component CI headquarters;

- The CISP will be reviewed annually, or as required by events. It will be used as the baseline for any evaluation of the program or facility and its supporting CI program; and

- Any updated CISP is redistributed to those providing support.

8.5.2.1. CI Actions at RDT&E Activities

Component CI agencies have identified a core listing of CI services that are recommended for each CISP.

- If there is DS&TI at a RDT&E site, the site director-approved CISP is provided to the DoD Component CI specialists working at the RDT&E site;

- If there is CPI at a RDT&E site, the program manager-approved CISP is provided to the DoD Component CI specialists working at the site and will become an annex to the site CISP;

- If DS&TI or CPI is identified at a DoD contractor facility, the program manager, CI specialist, the DSS CI specialist, and the contractor develop a CISP annex to define CI support to the contractor; and

- If RDT&E site management identifies DS&TI or CPI requiring specialized CI support beyond what is covered in the project or program CISP, that additional support is documented as an annex to the site CISP.

Component CI personnel keep the project or program manager CI POC informed of threat and other information that could adversely impact the DS&TI or CPI. The CI POC is responsible for keeping the program manager or site director apprised of current CI activities.

When more than one Component CI agency has an interest at the same RDT&E site or contractor facility, teaming, and cooperation should occur at the lowest possible organizational level. If a conflict occurs that cannot be resolved by the DoD Components, information on the conflict is sent to the Deputy Undersecretary of Defense (Counterintelligence and Security), OUSD(I), for review and resolution.

8.5.2.2. Counterintelligence Support to Acquisition Programs

Component CI organizations should identify a CI specialist to acquisition program managers with CPI. The CI specialist should:

- Participate in the RTP WIPT that develops the PPP and is responsible for developing the CISP and obtaining the MDCI Threat Assessment for the program;

- Ensure CI RTP requirements flow to CI and security personnel at locations where the CPI is used, handled, stored, or tested;

- Ensure the program manager and the program office staff are aware of current threat information; and

- Provide specialized CI support to all locations pursuant to the CISP.

Field CI personnel should:

- Provide CI RTP support when the weapons system or other platform becomes operational for as long as CPI is designated; and

- Provide CI support for as long as the CPI is so designated.

8.5.3   Anti-Tamper

8.5.3.1 General

- Program managers should develop and implement Anti-Tamper (AT) measures to protect DS&TI and/or CPI in U.S. defense systems developed using co-development agreements; sold to foreign governments; or no longer within U.S. control (e.g., theft, battlefield loss). AT techniques may be applied to system performance, materials, hardware, software, algorithms, design, and production methods, or maintenance and logistical support. Although protective in nature, AT is not a substitute for program protection or other required security measures;

- AT adds longevity to a critical technology by deterring reverse engineering. AT also provides time to develop more advanced technologies to ensure previously successful hostile exploitation of a defense system does not constitute a threat to U.S. military forces and capabilities. Although AT may not completely defeat exploitation, it will make hostile efforts time-consuming, difficult, and expensive;

- AT is initiated as early as possible during program development, preferably in the program concept refinement and technology development phases, in conjunction with the identification of program DS&TI and/or CPI:

  o AT is also applicable to DoD systems during a Pre-Planned Product Improvement (P3I) upgrade or a deployed system technology insertion; and

  o Additionally, AT should be specifically addressed in all transfer or sales of fielded systems and in direct commercial sales to foreign governments.

- AT resource requirements may affect other aspects of a program, to include end item cost, schedule, and performance;

- AT also involves risk management. A decision not to implement AT should be based on operational risks as well as on acquisition risks, to include: AT technical feasibility, cost, system performance, and scheduling impact;

- The DoD Executive Agent for AT resides with the Department of the Air Force, which is responsible for:

    o Managing AT Technology Development;

    o Implementing Policy;

    o Developing an AT databank / library;

    o Developing a Technology Roadmap;

    o Providing Proper Security Mechanisms; and

    o Conducting AT Validation.

- The AT Executive Agent sets up a network of DoD Component AT points of contact to assist program managers in responding to AT technology and/or implementation questions. Additionally, DoD Component POCs coordinate AT development and create a shared common databank / library; and

- Since AT is a systems engineering activity, AT is strengthened when integrated into a program sub-system(s), and is more cost effective when implemented at program onset.

8.5.3.2. Application of AT

- With the aid of the DoD Component AT POC, the program manager should determine the appropriate number of AT layers to be employed on the program using a risk assessment of the CPI. The evaluation may indicate there is no requirement to apply AT techniques. However, a final decision should not be made until completing thorough operational and acquisition risk analyses;

- AT applicability should be assessed for each major modification or P3I upgrade to the production system and for any FMS of fielded systems or direct commercial sale. It is feasible that AT may be inserted into the modified or upgraded systems when protection is required. AT may be discontinued when it is determined the technology no longer needs protection; and

- The program manager recommendation whether or not to implement AT should be approved by the Milestone Decision Authority and documented in the Program Protection Plan (PPP).

8.5.3.3. AT Implementation

- The program manager should document the analysis and recommendation in the classified AT plan (an annex to the PPP), of whether or not to use anti-tamper measures. The PPP with the AT annex should be included in the submission for Milestone B, and updated for Milestone C. The AT Executive Agent, or any DoD

Component-appointed AT Agent, provides an evaluation of the AT plan and a letter of concurrence to the Milestone Decision Authority;

- The AT classified annex to the PPP contains AT planning. The planning detail should correspond to the acquisition phase of the program;

- The AT annex includes, but is not limited to, the following information:

    o Identification of the critical technology being protected and a description of its criticality to system performance;

    o Foreign Teaming and foreign countries / companies participating;

    o Threat assessment and countermeasure attack tree;

    o AT system level techniques and subsystem AT techniques investigated;

    o System maintenance plan with respect to AT;

    o Recommended solution to include system, subsystem and component level;

    o Determination of how long AT is intended to delay hostile or foreign exploitation or reverse-engineering efforts;

    o The effect that compromise would have on the acquisition program if AT were not implemented;

    o The estimated time and cost required for system or component redesign if a compromise occurs;

    o The program manager recommendation and the Milestone Decision Authority decision on AT; and

    o The program AT POC.

- AT is reflected in system specifications and other program documentation; and

- AT, whether implemented or not, should be a discussion item during Milestone B, Milestone C (Low-Rate Initial Production), and Full-Rate Production Decision Reviews:

    o At Milestone B, the program manager should address AT in conceptual terms and how it is to be implemented. Working AT prototypes, appropriate to this stage of program development, should be demonstrated. Deliverables at Milestone B include: a list of critical technologies/information; a MDCI threat analysis; a list of identified vulnerabilities; identified attack scenarios; impacts if exploited; available AT techniques; and a preliminary AT Plan. These deliverables are submitted and incorporated into the AT Annex of the PPP; and

    o At Milestone C, the program manager should fully document AT implementation. Deliverables at Milestone C include: all deliverables from Milestone B and any updates; an analysis of AT methods that apply to the system, including cost/benefit assessments; an explanation of which AT methods will be implemented; and a plan for verifying and validating

(V&V) AT implementation. These deliverables are submitted and incorporated into the AT annex of the PPP. Testing during developmental test and evaluation (DT&E) and operational test and evaluation (OT&E) is highly encouraged for risk reduction.

8.5.3.4. AT Verification and Validation (V&V)

AT implementation is tested and verified during DT&E and OT&E.

The program manager develops the validation plan and provides the necessary funding for the AT V&V on actual or representative system components. The V&V plan, which is developed to support Milestone C, is reviewed and approved by the AT Executive Agent, or any Component-appointed AT Agent, prior to milestone decision. The program office conducts the verification and validation of the implemented AT plan. The AT Executive Agent witnesses these activities and verifies that the AT plan is implemented into the system and works according to the AT plan. The program manager and the AT Executive Agent may negotiate for parts of the system that have undergone anti-tamper measures to be tested at the AT Executive Agent's laboratories for further analysis. The validation results are reported to the Milestone Decision Authority.

8.5.3.5. Sustainment of AT

AT is not limited to development and fielding of a system. It is equally important during life cycle management of the system, particularly during maintenance.

AT measures should apply throughout the life cycle of the system. Maintenance instructions and technical orders should clearly indicate that AT measures have been implemented; indicate the level at which maintenance is authorized; and include warnings that damage may occur if improper or unauthorized maintenance is attempted. To protect CPI, it may be necessary, as prescribed by the DDL, to limit the level and extent of maintenance a foreign customer may perform. This may mean that maintenance involving the AT measures will be accomplished only at the contractor or U.S. Government facility in the U.S. or overseas. Such maintenance restrictions may be no different than those imposed on U.S. Government users of AT protected systems. Contracts, purchase agreements, memoranda of understanding, memoranda of agreement, letters of agreement, or other similar documents should state such maintenance and logistics restrictions. When a contract that includes AT protection requirements and associated maintenance and logistics restrictions also contains a warranty or other form of performance guarantee, the contract terms and conditions should establish that unauthorized maintenance or other unauthorized activities:

- Should be regarded as hostile attempts to exploit or reverse engineer the weapon system or the AT measure itself; and

- Should void the warranty or performance guarantee.

The U.S. Government and U.S. industry should be protected against warranty and performance claims in the event AT measures are activated by unauthorized maintenance or other intrusion. Such unauthorized activities are regarded as hostile attempts to exploit or reverse engineer the system or the AT measures.

8.5.3.6. Guidelines for AT Disclosure

The fact that AT has been implemented in a program should be unclassified unless the appropriate original classification authority of the DoD Component, in consultation with the program Milestone Decision Authority, decides that the fact should be classified.

The measures used to implement AT will normally be classified, including any potential special handling caveats or access requirements. The AT implementation on a program should be classified from SECRET / US ONLY (minimum) to SECRET / SAR per the AT security classification guide. Classified AT information, including information concerning AT techniques, should not be disclosed to any unauthorized individual or non-U.S. interest pursuant to decisions made by appropriate disclosure authorities.

Disclosure decisions should take into account guidance and recommendations from the program OCA, in consultation with the program Milestone Decision Authority, and those of USD(AT&L). The program Milestone Decision Authority coordinates all foreign disclosure releases involving AT with the cognizant foreign disclosure authority and security assistance office, as appropriate. An exception to National Disclosure Policy may be warranted for co-development programs, foreign military sales, or direct commercial sales.

8.5.4. Information Assurance

All information systems (including network enclaves) storing, processing, or transmitting DS&TI must comply with the requirements of DoD Directive 8500.1 "Information Assurance (IA)" and implement the appropriate IA controls from DoD Instruction 8500.2 "Information Assurance Implementation". Accordingly, these systems will be accredited in accordance with DoD Instruction 5200.40 "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)". The DITSCAP establishes a standard process, set of activities, general task descriptions, and a management structure to certify and accredit IT systems throughout the system life cycle. A product of the DITSCAP, the System Security Authorization Agreement (SSAA), documents the agreement between the project manager, the Designated Approval Authority (DAA), the Certification Authority (CA), and the user representative concerning schedule, budget, security, functionality, risk, and performance issues. Applicable SSAAs will be included as annexes to the PPP. Associated costs will be recorded in the PPP by fiscal year. For information systems where the program office is not the owner of the system but simply a user of the system, the PPP should include a copy of the system's Approval to Operate (ATO) issued by the system DAA.

It is important to differentiate between the implementation of information assurance with regards to program support systems processing DS&TI and other CPI, as opposed to the implementation of information assurance in the system being acquired. For example, a hypothetical acquisition program office acquiring a new weapons system (or AIS) may have an information system that supports the storing, processing and transmitting of DS&TI. The information assurance requirements and certification and accreditation requirements for that support system are totally separate and distinct from those of the weapons system being acquired. Chapter 7, Acquiring Information Technology and

National Security Systems, provides specific guidance on the identification and implementation of information assurance requirements for all systems being acquired.

8.5.5. Horizontal Analysis and Protection

The objective of horizontal analysis and protection activities is to ensure consistent, cost-effective application of similar RTP safeguards for similar DS&TI and/or CPI throughout DoD.

- CIFA conducts horizontal analysis to determine whether similar technologies are being used in different programs;

- Program managers, Program Executive Officers, and Milestone Decision Authorities should assist in these analyses to ensure that similar technologies are safeguarded with the same level of protection, (i.e., horizontal protection); and

The USD(I), the USD(AT&L), and the DOT&E provide oversight of the effectiveness of horizontal analysis and protection as outlined in DoD Directive 5200.39.

8.5.5.1. Horizontal Analysis

The CIFA-conducted horizontal analysis should address the following:

- System enabling technologies (DS&TI and/or CPI) and their additional applications, whether for similar or dissimilar tasks;

- RTP safeguards planned or provided;

- Intelligence estimates of competitive foreign acquisition efforts; and

- Reports of completed investigations of compromises, espionage cases, and other losses.

DoD Components should establish processes that support horizontal analysis and protection activities. DoD Components should:

- Identify system enabling technologies and their additional applications, whether for similar or dissimilar tasks;

- Review security classification guides of existing programs or projects when developing a CISP or PPP to determine classification of similar technologies used in other programs or under development.

- Catalogue, analyze, group, and correlate protection requirements within approved PPPs or CPI for DS&TI involving similar enabling technologies. Provide the data collected to the CIFA for their use.

8.5.5.2. Horizontal Protection

CIFA will provide their analysis report to the site director for emerging technologies and/or to the program manager for their application within an acquisition program. Site directors or program managers should ensure their respective CISP and PPP are modified when required based upon results of the horizontal analysis.

CIFA will coordinate all reported or discovered discrepancies with the appropriate DoD Components for resolution at the lowest possible organizational level.

When necessary, CIFA will report unresolved or inconsistent applications of RTP safeguards to the USD (AT&L), DOT&E, and USD (I) for resolution. Copies of these reports will be provided to the DoD Inspector General (IG).

8.5.5.3. Reporting Requirements

Compromise of DS&TI or CPI will be reported through CI channels to CIFA and the USD(I), in accordance with DoD Instruction 5240.4

8.5.6. RTP Assessments and Inspections

Periodic assessments and inspections of RTP activities (encompassing all DoD RDT&E budget categories) are necessary to ensure effective RTP is being planned and implemented. The DoD Component responsible for the RDT&E site or the acquisition program is responsible for these assessments and inspections (DoD Directive 5200.39).

8.5.6.1. Assessments

DoD Components periodically assess and evaluate the effectiveness of RTP implementation by RDT&E site directors and program managers as well as the support provided by security, intelligence, and CI to RDT&E sites and acquisition programs with DS&TI or CPI.

8.5.6.2 Inspections

The DoD Inspector General (IG) has established a uniform system of periodic inspections, using the existing DoD Components' inspection processes for RDT&E sites, to ensure compliance with directives concerning security, RTP, and CI practices.

The DoD IG has developed RTP inspection guidelines for use by DoD and DoD Component Inspectors General to enhance consistent application of directives that apply to RTP directives and related issuances.

DoD Component IGs conduct periodic inspections, using the DoD IG inspection guidelines, of RDT&E sites and acquisition programs for compliance with RTP directives. These inspections assess program manager compliance with section 8.4.11.2, Assessment of PPP Effectiveness. Participating Inspectors General may modify or customize the DoD IG inspection guidelines to account for Military Department-specific approaches to security, technology protection, and counterintelligence.

The DoD IG conducts periodic audits of DoD Component IG inspections for compliance with RTP directives and related issuances.